James Dean

November 16, 2020

Transmute Industries

Decentralized Identifiers & Verifiable Credentials

Every modern identifier is tied to a centralized entity. While that might not sound conflicting with respect to basic standards for verifying one's identity, individuals typically sacrifice personal data as means to confirm their asserted claims. This poses a threat to the users' information considering each method of identification is an independent entity. For example, every time you take a new job or open a new bank account in the United States, the subject is required to give out their social security number. This requires a significant amount of trust. Not to mention malicious actors that pose to benefit off this system, from the minor trying to buy alcohol at a gas station to the senior whose identity is stolen when they need social security benefits to get by. The lack of a trustless universal protocol hinders our ability to effectively certify claims without sacrificing vulnerable information. Decentralized Identifiers & Verifiable Credentials, through implementation of cryptography and distribution, provide a safe medium for confirming claims without risking essential data and creates a trustless validation system that operates at scale. Essentially this development allows possibilities such as, a Canadian citizen proving their residence status without giving away the location of their home, or even instantaneously confirming the status of immunologist in Berlin seeking medical records for a virus in Wuhan.

With respect to Verifiable Credentials, it’s essential to understand what it means to assert a claim along with the implication of doing so on the internet. If a Canadian citizen needs to prove their status as a resident, they could present a passport. In this case, the subject is the

citizen, the value being their home address, and the claim would be that this address is in fact where they live. However, backing up this claim through the internet, as mentioned by W3C, “makes it challenging to receive the same benefits”. This is where Verifiable Credentials come into play. An issuer can create a verifiable credential based off of asserted claims and transmit such credential to the subject of the claim. Therefore, when the subject of the claim receives a verifiable credential from the issuer, the subject is a holder of such credential and can generate verifiable presentations containing “data that is synthesized from the original verifiable credentials” (W3C). This data is secure throughout the process, using distributed ledger systems such as a blockchain, because it’s encoded and requires cryptographic verification to be accessed. In the case of our Canadian citizen, the entity that sold the house to the citizen could subsequently issue a verifiable credential to the resident. This would allow the resident, when prompted to prove citizenship, to submit their credential to a verifier who can then confirm the holder's status as a Canadian citizen without actually seeing any of that personal metadata being staked. To illustrate this process I made a diagram, Figure 1, that highlights the relationship between issuers, holders, & verifiers. The verification process requires an actor, known as the

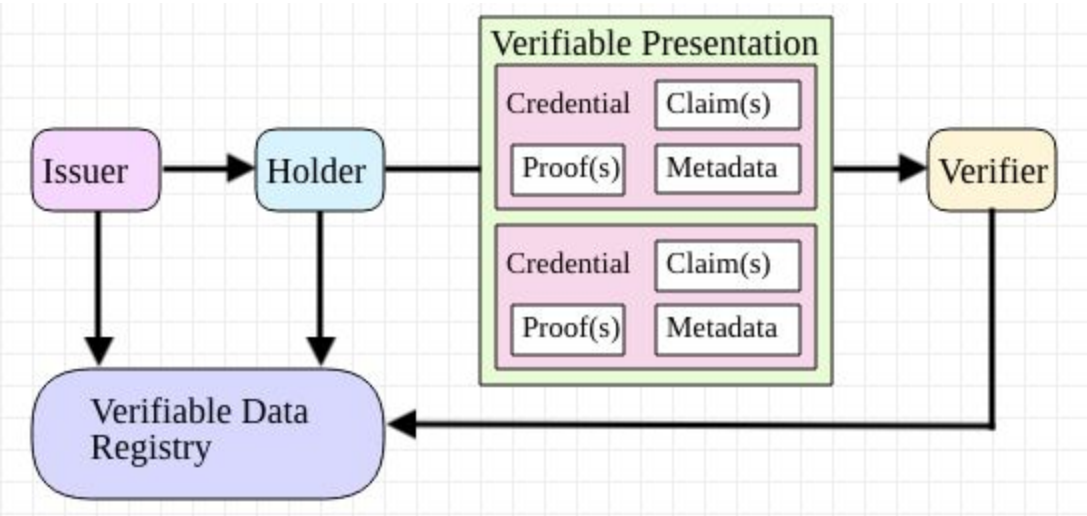

Figure 1

verifier, to receive a credential or presentation. Then the verifier checks that the credential or presentation conforms to specification and satisfies the proof. This is done securely using digital signatures along with private & public keys. Another significant role in this process is one of verifiable data registries that mediate the creation and verification of credentials, to maintain security in a trustless system, it's best to implement such registries using a public blockchain.

Conversely, Decentralized Identifiers "enable individuals and organizations to generate our own identifiers using systems we trust" (W3C). This is different from verifiable credentials in the sense that we can create our own identifiers as opposed to being sent one by an issuer. Although, using cryptographic proofs like digital signatures and biometrics, we can still authenticate the security of each decentralized identifier we're associated with. While a DID subject is the person or group that's identified by the DID, the DID controller "has the ability to make changes to a DID document" (W3C). The difference between the subject and controller is significant because in most cases the subject is the controller, although this relationship is not required. Furthermore, the DID controller has the ability to grant permission to a DID delegate so they can authenticate the identifier using verification methods. To illustrate the syntax of a DID and its respective document, a sample DID document, implemented by Orie Steele at Transmute Industries, is provided in figure 2.

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    {
      "@base": "did:web:did.actor:bob"
    }
  ],
  "id": "did:web:did.actor:bob",
  "publicKey": [
    {
      "id": "#z6MkkQBvgvqb6zGvS4cydworpUaRDzpszSFixq49ahbDeUTG",
      "type": "Ed25519VerificationKey2018",
      "controller": "",
      "publicKeyBase58": "6wvt6gb9mSnTKZnGxNr1yP2RQRZ2aZ1NGp9DkRdCjFft"
    }
  ]
}
```

Figure 2

Essentially, a DID URL can be dereferenced using resolution methods “to fetch a DID document indicated by the DID contained in the DID URL” (W3C). Within the DID document, as seen in figure 2 (Steele, Transmute), we see public keys that’re used to prove the documents association to the DID through verification methods. An example of a DID URL, implemented by Orie Steele at Transmute Industries, is `did:key:z6MkpP568Jfkc1n51vdEut2EebtvhFXkod7S6LMZTVPGsZiZ`. Significantly, the user holds the DID “which is mapped to [a DID document] stored in a registry” (Alzahrani, IEEE). This data is secure considering the registry is implemented on a distributed ledger, such as a blockchain, where access is only granted by providing a biometric or private key associated with the public key.

With respect to Decentralized Identifiers & Verifiable Credentials, while both can be implemented and used individually, our best chance at achieving true decentralization is through the implementation of both technologies in the same system. For instance, a verifiable credential, associating claims to a subject, must contain a property in its data that represents the credential subject. While it’s not required, a decentralized identifier could satisfy the need for subject representation in a credential. Many developers have implemented smart contracts that stage elections online using blockchain technology. Currently mis-information about voting is at an all time high, although elections using blockchain technology are widely disregarded due to complexities with confirming citizenship status and ensuring each eligible voter only votes once. Using verifiable credentials and decentralized identifiers provides the means to confirm an individual's status as a citizen, thus allowing the possibility to safely use smart contract elections without the implication of fraudulent activity. Decentralized Identifiers & Verifiable Credentials provide a trustless validation system that operates on a global scale. The lack of a trustless universal protocol hinders our ability to effectively certify claims and still guarantee validity.

Works Cited

Alzahrani, B. "An Information-Centric Networking Based Registry for Decentralized Identifiers and Verifiable Credentials." *IEEE Access, Access, IEEE*, vol. 8, Jan. 2020, pp. 137198–137208. *EBSCOhost*, doi:10.1109/ACCESS.2020.3011656.

Reed, Drummond, et al. "Decentralized Identifiers (DIDs) v1.0." *W3C*, World Wide Web Consortium, 2020, www.w3.org/TR/did-core/.

Sporny, Manu, et al. "Verifiable Credentials Data Model 1.0." *W3C*, World Wide Web Consortium, 19 Nov. 2019, www.w3.org/TR/vc-data-model/.

Steele, Orie. "Transmute-Industries/Vc.js." *GitHub*, Transmute Industries, 2020, github.com/transmute-industries/vc.js.

Steele, Orie. "Transmute-Industries/Did.actor." *GitHub*, Transmute Industries, 2020, github.com/transmute-industries/did.actor.